国家安全保障科学技術局の設立を！

～経済安全保障戦略の拡充と加速を～

2022年3月16日

技術安全保障研究会

目　次

（はじめに　経済安全保障の重要性の高まり）

１ ロシアのウクライナへの軍事侵略

本年２月ロシアはウクライナに軍事侵略を始めた。国際法に違反する暴挙だ。

自由民主主義陣営（西側）の諸国は、SWIFT（国際銀行間通信協会）からのロシアの排除を始め、幅広い分野で制裁措置を導入した。侵略を受けたウクライナと同盟諸国の安全保障を経済的手段によって図る、経済安全保障の時代が劇的に視角化されたのである。これに対し、ロシアも対抗措置を講じている。これにより、世界経済は、金融・エネルギー・食糧・物流など全面的にロシアと西側諸国が分断された。グローバル化一辺倒の時代は終焉を遂げ、「鉄のカーテン」と「ブロック経済」が復活しつつある。日本は、エネルギーも食料も海外依存度が高いため、安全保障に重大な影響が生じている。

２ 米中対立は激化し長期化する見込み

米国では、バイデン大統領はトランプ大統領時代の対中制裁を継続するともに、人権侵害をも理由に対中制裁を拡大してきた。また、中国の台頭への対抗軸を民主主義対専制主義の戦いと捉え、同盟国に協力を働き掛けてきた。

中国は、米国の制裁に対する対抗法を制定した。自立自強で独自技術開発に注力し、今世紀半ばには中華民族の偉大な復興を遂げることを目標にしている。

この基調は、ロシアのウクライナ侵略によって強まりこそすれ、弱まることはない。2021 年の念頭にはわが国でほとんど意識されていなかった「台湾有事」が、いまや現実のものとして各界有識者に意識されている。欧州で起こった破局的シナリオが東アジアで再現しないようにすることが、我が国の政策の第 1 優先課題である。

３ コロナ禍の発生

コロナ禍の発生は、我が国の経済安全保障に大きな問題を引き起こした。

第１に、ワクチン・治療薬の不足だ。日本は医薬品の国内開発路線をとってきたが、実力不足が明らかになり、全面的に米欧からの輸入に依存せざるを得ない状況である。このため外国の製薬企業や外国政府の輸出管理に翻弄されている。

さらにマスク、医療用品などのローテク製品を含め中国への依存が高く、国内の供給不足により、社会不安が発生した。

第２に、グローバルサプライチェーンの途絶だ。外国に依存していた部品や素材の輸入が止まり、国内の工場が停止した。製品の輸入不足で国民生活も混乱に陥った。

４　科学技術力の強化が最重要課題

「科学技術力なくして安全保障なし」

残念ながら、日本の科学技術の国際競争力は低下し続けている。科学技術力の強化が安全保障の最重要課題だ。科学技術力は、経済的繁栄の基礎であると同時に、防衛力を支える。また科学技術分野は、「効率的」で「安定」した権威主義的体制との比較において、自由民主主義陣営が明確な優位を有する領域である。

「安全保障なくして企業活動なし」

民間企業の活動は、国家の安全保障が前提であり、安全保障戦略に適合し寄与することが求められている。経済安全保障に関しては、コスト高要因であるとして可能な限り回避しようとの論調も、一部に見られる。だが、米中の首鼠両端を持してうまく立ち回ればよいというのは、楽観的に過ぎる。国の安全なくして安定した企業活動など営めないことを、今回のウクライナ侵略が劇的に明らかにした。

５　政府や自民党の経済安全保障への取り組みを高く評価

政府は、国家安全保障局に経済班を設置するとともに、首相が国会演説で経済安全保障に取り組むことを表明し、経済安全保障担当大臣を設置し、経済安全保障推進法案を国会に提出した。画期的な第一歩であり、早期成立と施行が強く期待される。

自民党は、新国際秩序創造戦略本部で総合的な提言をするとともに、経済安全保障対策本部に改組し、全党的に取り組んでいる。全世界的な危機ともいえる今日の状況において、その姿勢もまた、高く評価される。

（基本的考え方　　米欧中に伍しうる官民一体体制の形成を）

「経済安全保障政策」は、言うまでもなく、「国家安全保障戦略」の一環である。国際情勢の変化、とりわけ今回のロシアのウクライナへの軍事侵略や北東アジアの安全保障環境の急激な変化に照らし、今後の我が国国家戦略の基本的価値観を、「国家安全保障」に置く事が必要であり、その価値観に沿って経済政策全般・科学技術政策全般を再構築するところに、「経済安全保障政策」の今日的意義がある。

その観点から、今後の経済政策の運営にあたり、以下の諸点を強調する。

（1）今回のロシアのウクライナ軍事侵略に当たって、各国の民間企業は、各国政府の制裁措置に呼応して、投資抑制、生産停止、輸出停止など、経済活動の断絶を迅速に実行している。正に「政経一体」の行動である。「国家安全保障」とは政治も軍事も経済も一体的に対処するものである。この際、民間企業は、国際情勢の変化に対して常に「政経分離」で済ませようとの願望は捨てるべきである。私企業といえども、「政経一体」の考えの下、自らを厳しく律する姿勢が求められている。

（2）冷戦終結後の約 30 年間、「市場は善、国家は悪」との前提の下、我が国は、「規制緩和、民営化、小さな政府」を標榜した経済政策を推進してきた。これは、一方向的なグローバル化の潮流の下では意味があったが、いまや、時代が大きく転換した。政府規制を無条件に悪とする考え方を早期に転換し、米欧中に伍しうる「官民一体」の体制を形成して、「国力」の結集を図るべきである。
（3）そのように考えるならば、企業は、資本市場の短期的要求のプレッシャーに第 1 に応えようとする「新自由主義」的思考を脱却し、国家の将来を見据えた長期的観点に立って、民間の投資行動、経済行動を誘導することである。
（4）かつて多くの日本の企業は長期的視野に立って投資、研究開発を行ってきた。しかし、近年は、グローバル化の潮流の下で、米国ウオール街の要請に沿った株主優先、短期利益優先の短期的思考に長く馴染んで来ており、長期的視点に立って投資リスクを果敢に取るよう要求するのは難しい。そのため、当分の間、国がリスクテイカーの役割を果たす事が要請される。米欧では、安全保障環境の変化を見据え、投資助成など、既に踏み込んだ「安全保障産業政策」が実施されている。さらに中国では独自の強力な産業政策を進め、国際競争力を高めている。
（5）国は、投資助成に加えて、リスクテイカーとして、研究開発、教育、サイバーセキュリティを軸とするデジタルインフラの整備など、「未来への投資」を強化すべきである。そして、苦しい財政事情の中でこれを十全に果たすためには、聖域なき予算内容の再検討など、タブー抜きで議論を行うべきである

今回のロシアのウクライナ侵略により、１９８９年の東西冷戦の終結後に構築された世界経済秩序は壊されつつある。ロシアは新しいブロック経済に追い込まれるものと見られ、世界経済は相当な年月に亘り、混乱が続く恐れがある。

日本は技術・エネルギー・食糧を含む総合的な経済安全保障戦略を早急に策定する必要がある。

当研究会はこの一環として技術安全保障の観点から、下記の通り提言する。

提言１　国家安全保障科学技術局の設立

１　国家安全保障科学技術局（日本版 DARPA）の設立

安全保障は国家の根幹であり、現代においてその根幹をなすのは、最先端の科学技術の研究である。米国では、安全保障を目的としたリスクの高い研究開発を国防高等研究計画局（DARPA）が担い、それを社会実装する際にベンチャー企業に対して適切な資金援助を行い、さらに成熟した後の段階で安全保障を目的とした技術として国に戻すサイクルが確立している。

これを日本でも実現するために、安全保障研究を従来手がけてこなかった大学や公的研究機関とは別に、国家安全保障科学技術局（日本版 DARPA）を設立し、巨額の研究開発資金を投入し、社会実装のためのベンチャー育成までをもその責任とする。

２「経済安全保障型産業政策」を策定

（1）デジタル革命の進行や米中対立、さらにロシアによるウクライナ侵略により、新自由主義やグローバリズムの時代は終焉し、米欧中ともに国家として技術開発や産業の育成に力を入れている。

（2）日本も経済安全保障を実現するため総合的な産業・技術育成政策を策定し、官民が協力して実現することが必要である。今回の経済安全保障推進法案は、先端技術に関する官民協力やサプライチェーンの強化を図っているのは高く評価されるが、更に総合的な産業政策を樹立する必要がある。

（3）日本独自の技術力・産業力を高め、内外の市場を獲得し、米国等のリードユーザーとの連携を実現し、政府・自治体等による積極的採用につなげ、日本企業の経営基盤の安定化につなげることなどを目指す。

（4）当面の対象分野としては、量子、AI、バイオなどの先端技術分野、半導体、レアアースなど外国依存の高い分野、医薬品、医療物資など国民の生命健康に関する分野、外国へのエネルギー依存を改善するグリーン革命関連分野などが考えられる。

（5）諸外国の巨額の助成に照らし、日本も、資金、初期需要の確保、販売助成などで国際的に遜色のない助成策を講じることで国際競争での勝利を目指すべきである。

例えば神奈川県横須賀市に量子サイバー研究拠点を作り、１兆円程度の政府資金を注入することが考えられる。

３　データフリーフロー政策の見直し及び国によるデータセンターの構築

（1）「20世紀の資源は石油、21世紀の資源はデータ」と言われ、データは経済的にも国家安全保障上も、死活的に重要になっている。

（2）米国は、IT 企業（ビッグ・テック）が世界最強で世界中のデータを収集し、保管している。EU は GDPR(一般データ保護規則)により、個人データの域外流出を事実上規

制しているが、さらに産業データの域外流出法案を公表している。中国はデータの国外流出を管理するだけでなく、中国の IT 関連企業が国外からデータを多量に中国に流入させており、データ保管量は増加している。
（3）これに対し、日本は IT 関連企業の国際競争力は弱く、データの外国への流出が日本への流入に比べはるかに多い。
　このため、EU や中国の政策を参考に、現在のデータフリーフロー政策（DFFT)を見直し、個人データや産業データの国外移転を規制すべきである。
（4）デジタル空間であるインターネットには国境がなく、クラウドと呼ばれる仮想空間で構築されている。しかし、そのクラウドはハードウェアであるサーバー（コンピュータの集合体）の中に存在しており、物理的にサーバーが設置されている国家によって事実上管理されている。
　2021年に発覚した LINE 問題の例もあり、我が国としてもサーバーの国内設置を義務付けるべきである。
　特に国益に直結するデータの保管については、強力なファイアウォールを備えた政府クラウドの設置が必須であり、サーバーを保管するスパコンを使った大型データセンターを、国家として国内に複数、分散配置し、情報管理の一元化を図るべきだ。
（5）スマホのアプリ、ビデオ会議システムなども外国製が多い。安全保障の観点から総点検し、対策を講じることが必要だ。

4　バイジャパニーズ政策の採用と政府調達方式の改善

（1）バイデン政権のバイアメリカン政策を参考に、日本も経済安全保障上必要なものはバイジャパニーズ政策を採用する。
　このため、政府調達の一般競争入札に関する方針を見直し、経済安全保障上必要ある時は、指名競争入札や随意契約が出来るように会計法29条の3を改正する。
（2）今回の経済安全保障推進法案では民間の基幹インフラに関しては経済安全保障の観点から事前審査をすることとされているが、さらに広く取り組むことが必要だ。
　①府省庁ならびに政府関連機関が情報機器等の調達を実施する際には、技術情報の漏洩を防ぐため、同盟国の政府やインテリジェンス機関の動向を踏まえ、経済安全保障の観点を加味し、調達産品やサービスを決定する。
　②府省庁ならびに政府関連機関と情報共有等を行う企業に対しては、一定期間内にセキュリティ上課題のある機器を社内システムから撤去する等の対策を実施するよう求める。

提言2　経済安全保障を国家安全保障の中核に位置づけて官民挙げて推進

1　経済安全保障を国家安全保障戦略、防衛計画の大綱、中期防衛力整備計画に明記

（1）「国家安全保障戦略」改定の際は、国全体として経済安全保障に断固たる決意で取り組むことを表明する。

（2）それを受けて改定される「防衛計画の大綱」「中期防衛力整備計画」において、経済安全保障のために必要な法令の整備、要員や装備の確保などを記載する。

（3）日本の最先端技術を防衛技術に活かすため、国家安全保障会議設置法第2条1項3号に規定する「防衛産業等の調整計画の大綱」を作成する。

この大綱には、下記「提言7　防衛産業の集約と新分野の育成」を含める。

（4）デュアルユーステクノロジーの重要性が高まっているため、総合科学技術・イノベーション会議に防衛大臣を追加する。

2　内閣官房に経済安全保障推進本部を設置

国全体で経済安全保障戦略を進めるために、「経済安全保障基本法」を制定し、内閣官房に経済安全保障推進本部及び事務局を設置する。

なお、相当数の事務局員は国家安全保障局と兼務する。

3　地方自治体における経済安全保障を考慮することの法的根拠の制定

地方自治体が企業誘致や港湾、空港といった公共インフラの運用、大規模な工業団地の転用などを検討する際に、経済安全保障リスクを考慮した判断をするための法的根拠を制定する。

4　国家安全保障会議に対する民間評議会の設置

経済安全保障については、常に新たな課題が生じている。このため、経済安全保障戦略の立案・実施にあたっては、民間の知見を最大限活用することが不可欠であり、経済人、有識者による評議会を設置する。

同評議会には、経団連会長、日商会頭など、民間部門のリーダーが参加し、経済安全保障に関わる諸課題につき、積極的・能動的に調査・検討し、国家安全保障会議に対して提言や報告を行う。

5　機関投資家に対する安全保障を踏まえた投資基準の整備

機関投資家は資金調達面で安全保障環境の悪化に肩入れしてしまうリスクを回避すべきである。よって資産運用先の選定に際し、日本政府、同盟国、友好国において

安全保障の観点から懸念が示された外国企業をポートフォリオに組み入れることを禁じ、保有後にリスクが判明した場合は適切なタイミングで売却すべきである。

また、機関投資家は ESG（Environment 環境、Social 社会、Governance 企業統治）の G（ガバナンス）の重要な要素として各国の安全保障政策情報の収集体制や予見可能な政策に対する能動的な準拠計画など、組織的な即応体制が整備されているかどうかを評価基準に加える。

６ 経済安全保障に関する国民の理解と協力

経済安全保障を高めるためには国民の理解と協力が必要だ。

日本は平和な環境に慣れてきているが、世界ではロシアのウクライナ侵略に見られるように軍事的な紛争が生じており、日本周辺でも、ロシアに限らず、力により現状を変更しようとする動きが続いている。外国で発生した新型コロナにより、国民の生活は大きく制約を受けている。サイバー攻撃は企業だけでなく身近な病院も狙われ、市民が被害にあっている。自然災害も多発している。

このような軍事・非軍事のリスクが高まりにより、サイバー防衛を含め経済安全保障の重要性が急速に高まっていることを、国民に分かりすく具体的に説明し、国民の理解と協力を得ることが必要である。

提言３ インテリジェンス機能の強化

１ 官民のインテリジェンス体制の強化

（１）今後、経済安全保障戦略がうまく進むかどうかは、情報機能（インテリジェンス）次第であるが、日本は外国に比べ、組織的にも要員的にも不十分だ。

外国の機微な情報や意図を収集・集約・分析・共有・活用という一連の流れを省庁の垣根を越えて行うため、内閣情報調査室を「局」に格上げするするとともに、内閣情報会議及び合同情報会議を強化する。

（２）諸外国の例を参考に、外国政府との関係の維持・強化を任務とする外交機関とは別に、外国の動向を冷静に把握・分析し、必要な警戒を行うために必要な根拠法と組織を整備する。

あわせて外交官でも警察官でもない「インテリジェンス・オフィサー」を、国として組織的に育成する。

（３）民間企業においてもインテリジェンス機能が重要になっているため、全社的な経済安全保障委員会（仮称）を設置し、政府機関との連携を図ることを推奨する。

２ 安全保障関連技術の専門研究組織の創設

インテリジェンス機能を高めるため、安全保障関連技術に関する研究組織（シンクタンク）を創設する。同組織は、ニーズを踏まえて科学技術を活用した解決策を研究する調査分析センターと、シーズとして世界の先進技術研究の状況を調べ、関連専門人材をネットワーク化しそのデータベースを構築するためのデータセンターで構成する。

政府から独立した非営利公益法人とし、運営は政府資金で行う。科学的分析に基づく中立的な立場での調査研究及び政策提言を行う。

セキュリティクリアランスについても考慮して、研究員として安全保障専門家、防衛省 OB、防衛企業経験者、大学関係研究者などを活用する。

３ 企業等への情報提供体制の構築

大企業のほか中小企業、都市部のほか地方部の企業にも世界に誇る先端技術が保有されている我が国の現状に鑑みると、懸念国による技術窃取の手口や有効な対策を全国に幅広く浸透させる必要があり、民間企業からインテリジェンス機関への積極的な情報提供を促す必要もある。そこで、関係する官公庁や十分な知見を有する民間事業者・団体によって、最新情勢を反映させながら定期的かつ網羅的に情報提供が推進されるような体制を構築すべきである。

なお、必要に応じ、メンバーシップを限定した情報提供の枠組みも創る。

４ 技術流出トラブルからの研究者の防護

大学や公的研究機関の研究成果が海外に流出するのを避けるため、研究室や個々の教員・学生・研究者からの自発的な申し出により、我が国のインテリジェンス機関との間で、平素から緊密に情報を共有することを可能にする体制を整備する。

また、そのように緊密な情報共有の対象となった教員･学生･研究者が、米国などの外国において、懸念国への技術流出に関わるトラブルに巻き込まれた場合には、適切な措置が執られるよう、日本政府として当該外国政府に働きかける。

提言４ 重要インフラの防護とサイバーセキュリティの強化

１ 重要インフラ防護体制の整備

（1）懸念国は、軍事的な攻撃の前に、電力や電気通信などのインフラに対して、サイバー攻撃による機能停止に追い込み、あるいはテロ攻撃により物理的な破壊を行うことを図る可能性が高い。重要拠点となる電力施設は１か所でも攻撃を受けるとカスケード障害という連鎖的な機能停止や破壊が起こる。将来はドローンによる攻撃も考えられる。

（2）日本では、重要インフラ防護は各省庁が担当しており、国全体の総合的な防護対策は十分ではなく、早急に総合的な防護体制を整備する必要がある。

①重要インフラのサイバーセキュリティ対策の徹底
防衛産業セキュリティ基準と同等の基準（SP-800）による自衛隊・警察との連携、重要インフラ事業従事者のセキュリティクリアランスの取得。

②ドローン攻撃・EMP(車載式)攻撃などの監視・防衛策

③サプライチェーン対策の徹底
防衛省が今後実施するサプライチェーン対策と同様の基準により、懸念国の会社やソフト・ハードの、下請会社からの排除。

④重要インフラへのサイバー攻撃及びテロ攻撃（物理的破壊工作）に関し、防衛省・警察を中心として、全省庁が協力したシミュレーションの実施

2　国全体のサイバーセキュリティ体制の強化

（1）2021年10月、徳島県の町立病院がサイバー攻撃を受け、本年2月にはトヨタの国内の全工場が操業停止に追い込まれるなど、今やサイバー被害は大企業だけでなく、身近なところで発生している。外国では石油パイプライン、重要拠点となる電力施設、銀行などのインフラも狙われている。攻撃者は政府系、非政府系など様々である。

（2）サイバー防衛は、個々の企業、組織、個人の対策だけでは不十分であり、日本も外国と同様に、国を挙げて次の対策を講じる必要がある。

①自衛隊法を改正し、自衛隊にサイバー防衛の任務を供与する。主要国の軍隊の例を参考に、自衛隊の位置づけと役割を明確にし、要員や装備を急速に増強する。

②電気通信事業法第4条を改正して、サイバーに対する積極防衛のため外国との間の通信調査を可能とする。

③アトリビューション（サイバー攻撃の実行者の特定）を可能とするよう法令を整備する。

④サイバー攻撃を受けた企業が速やかに政府に報告する制度を作る。これにより、政府は、被害の拡大を防ぐとともに、同種事例の予防策を講じることが出来る。

3　重要インフラにデジタルプラットフォーマー・物流センターを追加

（1）一定規模の個人情報を保有するデジタルプラットフォーマーを重要インフラ事業者に指定し、政府の指導に従わない、または指導しても是正されない場合には営業・業務停止を強いることが可能な管理下に置くべきである。

（2）物流センターはこの数年の間に配送情報だけでなく、個人情報や製品の図面データを有し、3D プリンターを用いた製造現場化も進み、多様な産業のデータの保有量

が増大している。また、自動化に伴う AI を活用したマテリアル・ハンドリング機器の海外依存度が増大し、サイバー攻撃による混乱が国民生活におよぼす影響が高まっている。このような物流センターを、重要インフラに指定すべきである。

4　セキュリティクリアランスの強化

（1）国家的に重要な先端技術の研究開発に民間の研究者や有識者が参画する機会が増大し、国際共同研究や開発などにおいて同盟国・友好国との間で秘密情報を共有する必要性が高まっている。

（2）今やほとんどすべての機器がインターネットにつながり、AI でコントロールされている。このため、デジタル関連の機器は、防衛システムだけでなく、一般民生機器においても、開発する人、製造する人の信頼性（トラスト）、セキュリティクリアランスが必要となっており、対策が求められている。

（3）先端技術のほとんどは、軍用・民生技術に境界のないデュアルユースである。防衛産業に留まらず、安全保障に関与する民間関係者の対象が広がりつつあるため、いわゆる「産業セキュリティ」（民間企業・機関をカバーする秘密保全および所属者個人に対するセキュリティクリアランス）の体制を早急に強化すべきである。

①政府横断的な産業セキュリティ規定の制定と一元的な責任組織の明確化
②先端技術・機微情報の対外共有・保全に係る専門性の提供と保全政策
③保全措置（人的背景調査、適格性審査、教育訓練、資格付与）実施機関の設置
④米国等と GSOMIA 付属文書として産業セキュリティ協定(ISA)を締結

提言５　経済安全保障法制の整備

1　新たな公益通報制度の創設と政府調達の仕組みの改善

（1）全ての産業において、経済安全保障リスクを高める恐れのある企業活動（情報管理、業務委託、資本や人的関係、ガバナンスなど）が確認された場合にその会社の役員、社員、契約社員、派遣社員もしくは2年以内にこれらの雇用形態にあった人物、当該企業とのビジネス取引を有する企業の役員または社員からの通報を受け付ける窓口を創設する。

当該窓口に寄せられた情報は全て日本の経済安全保障を担うインテリジェンス機関と共有するとともに、業法を有する産業の場合は監督官庁と共有して事実確認と改善・指導を行える仕組みを構築する。

（2）あわせて、入札に偏った政府調達の仕組みを改め、新たな公益通報制度の対象となるものについては、入札によることなく調達が行えるようにする。（提言 1 の 4 と併せ、会計法 29 条の 3 を改正する。）その際、政府調達の対象について新たな公益

通報制度による通報を行った個人や民間企業に対しては、その功績に応じて手厚く報奨を支払う仕組みとする。

２ 営業秘密を窃取しようとする段階での検挙を可能とする不正競争防止法の改正

現状の不正競争防止法では、現実に情報を盗られた、あるいはその実行に着手していなければ検挙ができない。これを改め、営業秘密に限り、同盟国と可能な限り同等な仕組みを目指し、窃取行為を共同で企画し秘密流出の危険性を発生させた段階で検挙できる仕組みに改正する。

３ コンサルティング業界に関する業法の制定

コンサルティング業界は日本企業の競争優位に関する情報だけでなく、近年は企業が保有する顧客情報の分析を委託されることで個人情報も保有し始めている。その上、アジア地域での統合がトレンドになっており、経済安全保障リスクが高まっているが、業法が無いためにこれを理由とした監査や業務停止などの行政指導が行えていない。これに対処するため、経済安全保障リスクを理由に業務停止を命じられる根拠法となる業法を創設する。

提言６ 経済安全保障を確保するための対外政策

１ 安全保障例外の外国並みの運用

（1）WTO（世界貿易機関）は、GATT（関税及び貿易に関する一般協定）21条の安全保障例外規定により、安全保障の観点からの規制・管理を当然のこととして認めており、多くの国は安全保障を考慮した通商政策を採っている。

（2）しかしながら、日本は、1995年のWTO発足時には経済の絶頂期にあったため、経済安全保障の観点のない純粋な自由貿易主義を採用し、国内法上の制限措置が極めて限定されたままとなっており、国際情勢の変化に対応していない。

（3）米欧や中国を参考に、自由貿易の原則を維持しつつも、経済安全保障の観点を加味して、平時から輸出入状況をモニターするとともに、物資需給上及び安全保障上必要なときは輸出入や投資の管理を行いうるよう、必要な法令を予め整備する。

（4）米国は法律や大統領令などを機動的に制定・改正して、輸出や投資の管理、政府調達からの排除、機微技術管理、経済スパイ対策などの制裁措置を講じている。中国はこれに対抗して、輸出管理法を施行し、信頼できない実体リストや輸出管理リストを公表するとともに、反外国制裁法を施行し、対象となる米国の個人・団体を発表した。EUでは「第3国による強制的措置の防止及び対抗措置に関するEU規則」の検討を開始した。

日本も、米国、中国、欧州の例を参考に、同種の報復法を整備する必要がある。

２　産業データの所有権及び情報管理のルール形成の推進

世界中で利用されている日本企業の製品から得られる個人情報以外の“産業データ”に関して所有権や情報漏洩時のルールは整備されていない。このまま行けば、産業データが全て個人データと同様の扱いがされてしまい、日本企業が情報を得るために個人から許可を得ることが必要となりコストが増加することが懸念される。日本企業のコスト負担が高まらず、データを利活用し易くなるようなルール形成を日本がリードすべきだ。

３　対象国の経済活動に関する政治的ガバナンスの状況評価とこれに応じた国際連携のレベル調整

企業活動、知的財産等に直接関連する制度・諸規制のみならず、民間保有データへの政府・政治のアクセスの状況、さらには民間保有データの国際的な移転の自由度などによって、各国の経済活動に関する政治的ガナバンスの状況を評価し、この評価に合わせて国際連携のレベルを設定するシステムを、米国等と協力し構築する。

４　人民武装部への企業の関与規制

中国共産党は外資企業に対しても予備役兵力である人民武装部の創設を指導しており、既に一部の日本企業の中国拠点において設置が確認されている。人民武装部は企業の人件費や経費によって運営されており、日本企業の資金が中国の軍事能力の向上に加担する構図となっている。

日本企業が外国の軍事力強化に協力するのを禁止・規制するなど、人民武装部の創設を拒否できるようにする根拠法を制定し、個別企業が中国共産党からの圧力を回避出来るようにする。

５　日米間での経営ガバナンスを議論するトラック 1.5 協議の創設

中国市場での活動を活発化し、サプライチェーンも依存したままの米国企業には、米国政府から問題視されるのを巧みに避けている例がある。そのためにどのような経営体制を構築しているのかは日本企業にとっても重要であるが、多くは合弁相手からですら把握できていない。よって米国企業の経営体制に関して情報を得るためのトラック 1.5 協議を創設する。

国際社会において、トラック 1 協議と呼ばれる政府間協議、トラック 2 協議と呼ばれる民間有識者間の意見交換に対し、最近はトラック 1.5 協議と呼ばれる政府職員と民間有識者が参加して行う意見交換が活発化している。本件は、政府と民間が情報を持ち寄り、一緒に対策を考えることが有効なので、トラック１．５協議が相応しい。

提言7　防衛産業の集約と新分野の育成

1　防衛産業の集約・国際化

（1）防衛産業への国内発注予算は減少し、防衛装備品の輸出は、事実上余り期待できないため、防衛事業から撤退する企業が続いている。

今の状況が続けば、5～10年後には日本の防衛産業は極めて弱くなり、防衛装備品の国内での保守・補修も難しくなる危機的な状況である。

（2）米国では防衛産業の再編が進み、日本の 10 倍以上の規模の市場に数社しか存在しない。欧州では、各国で分担し、各市場に欧州全体として 1 社しかない。

我が国では、防衛産業規模が小さいにも関わらず、防衛産業が大企業の一事業部門として存在していることなどから、冷戦終焉後、約30年を過ぎても、再編・集約は極めて限られたかたちでしか実現していない。

（3）わが国は、戦略的に防衛比率の高い企業を育成することが必要である。このため、政府として、調達先・契約先を集約させる方針を明確化し、これに沿った防衛力整備計画を策定し、業界の再編・集中を促すべきである。同時に、同盟国・友好国との防衛・安全保障関連の技術・産業協力を推進することが、わが国の安全保障に資することを政治的に明確化し、国際的な連携強化を推進すべきである。

また技術開発推進のため、大学やベンチャー企業の技術を取り込むべきである。経済安全保障推進法案が成立し、秘密特許制度（特許の公開制限）が実現した場合には、既存の防衛産業において活用し難い先端技術を国が取り込む窓口として制度を活用するため、公開制限に対する補償を充実すべきである。

2　新領域分野の防衛企業・人材の育成

サイバー、宇宙、電磁波、無人機などの新領域の防衛は今後益々重要になるため、新領域の防衛に必要な態勢（技術・装備・人材）を早急に整える必要がある。このため、優先的な予算配分を実施すべきである。

新領域は従来の戦車・自衛艦・戦闘機などとは異なった戦闘領域であるため、人材育成をはじめ、国内の技術生産基盤を育成することが重要であり、国策的にこの分野の防衛企業・人材を育成する必要がある。

3　災害対処産業の育成と災害対処予算の大幅増額

質的に多種多様な災害が多い日本において、自衛隊が積み上げて来た災害対処能力は国際的に高く評価されている。一方で、温暖化によって増加し続けている自然災害は、災害対処に自衛隊員の工数を大きく奪い、最近はそれを理由に予定されて

いた国際的な合同演習への参加を見送るなど、本来の任務である国防にも支障をきたし始めている。

今後も増加傾向が確実な災害対処活動と、昨今の自衛隊の採用で募集人員割れが続いている状況を踏まえると、災害対処活動をこれまでと同様に自衛隊員が行い続けることは、国防に必要な要員を確保するうえで障害となる。

よって災害対処活動を自衛隊がある段階から委託できる民間企業を災害対処産業として創り出し、戦略的に産業育成していくべきである。また、民間への委託を前提に、増加し続ける自然災害を織り込んで自衛隊の災害対処予算を大幅に増額することが必要である。災害対処を請け負う民間企業は効率的な業務遂行と質の高い災害対処を実現するために、資機材や復旧プロセスにて重要となる被災住民への衛生サービス、仮設住宅など実践経験に裏付けられた多様な製品・サービスを開発し、これらを質の高いインフラ輸出と連携して輸出していくことも視野に入れるべきである。

（参考）技術安全保障研究会について

座長	玉井克哉	東京大学教授・信州大学教授
委員	油木清明	BGA Japan 代表、戦略国際問題研究所(CSIS)ｼﾆｱｱｿｼｴｲﾄ
	荒井寿光	知財評論家、元通商産業審議官
	岩瀬充明	元警察庁生活安全局長
	兼原信克	同志社大学特別客員教授、元内閣官房副長官補
	國分俊史	多摩大学大学院教授・ルール形成戦略研究所長
	坂本吉弘	安全保障貿易情報センター理事長、元通商産業審議官
	長瀬正人	グローバルインサイト代表取締役社長、元三菱商事
	西　正典	元防衛事務次官
	西山淳一	未来工学研究所研究参与、元三菱重工業
	頓宮裕貴	サイバーセキュリティ有識者、元情報処理推進機構理事
	森口泰孝	JAEA シニアアドバイザー、元文部科学事務次官
	渡辺秀明	元防衛装備庁長官
事務局長	國分俊史	多摩大学大学院教授・ルール形成戦略研究所所長
幹事役	利光　尚	安全保障貿易情報センター参与、元三菱商事

技術安全保障研究会は、日本の技術・経済・安全保障に関する学界・官界・経済界の有識者により、2017年に設立され、内外の情勢分析や提言活動を行っている。

2018年10月10日　第1次提言
「諸外国並みの技術安全保障体制の構築を
～技術保護とサイバーセキュリティが急務～」
https://crs-japan.org/publications

2020年3月11日　第2次提言
「経済安全保障法の制定を」
https://crs-japan.org/publications/recommendation-economic-security-law/